УДК 681.3.06

О.О. Кузнецов, Р.В. Корольов, Ю.М. Рябуха

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

МЕТОД ШВИДКОГО ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ДОКАЗОВОЇ СТІЙКОСТІ

Розглядаються методи формування послідовностей псевдовипадкових чисел (ППВЧ), досліджується підхід до побудови доказово безпечних генераторів, стійкість яких обґрунтовується теоретико-складністною проблемою синдромного декодування. Пропонується метод швидкого формування ППВЧ доказової стійкості, який дозволяє забезпечити максимальний період формованих послідовностей. Проводиться дослідження стійкості запропонованого методу формування ППВЧ до криптографічних атак супротивника, заснованих на використанні алгоритмів декодування надмірних (n, k, d) кодів над GF(q)

Ключові слова: *послідовності псевдовипадкових чисел, генератор псевдовипадкових чисел.*

Вступ

Постановка проблеми в загальному вигляді і аналіз літератури. Методи формування ППВЧ доказової стійкості засновані на використанні односторонньої криптографічної функції: факторизації, дискретного логарифмування та ін. [1 – 8]. Основна перевага відповідних генераторів полягає у високих показниках статистичної безпеки [9]. Крім того, обчислення секретного ключа зводиться до добре відомої теоретико-складностної задачі, що обґрунтовує безпеку доказово стійких (Provably Security) генераторів [10].

У той же час слід зазначити загальний недолік відомих методів формування ППВЧ доказової стійкості – це надзвичайно висока обчислювальна складність, обумовлена необхідністю виконання математичних обчислень над дуже великими числами (порядку $2^{1000} – 2^{5000}$). Виняток становлять доказово стійкі генератори ППВЧ, обчислення секретного ключа в яких зводиться до розв'язання теоретико-складностної задачі синдромного декодування [5, 11]. У цьому випадку складність формування ППВЧ визначається процедурами кодування лінійних надмірних кодів, що зіставно по швидкодії з симетрич-

ним криптографічним перетворенням. Іншими словами, застосування генераторів ППВЧ на надмірних кодах дозволяє, з одного боку, забезпечити високі показники статистичної безпеки і можливість застосування моделі доказової стійкості, з іншого боку, реалізувати швидке формування ППВЧ [5, 11].

Доказово стійкий генератор ППВЧ на надмірних кодах (Generator Provably as Secure as Syndrome Decoding –GPSSD) вперше запропонований в [5]. У [9] досліджена його статистична безпека за методикою NIST STS і виконано порівняння з іншими генераторами ППВЧ. Встановлено, що показники статистичної безпеки генератора GPSSD значно перевищують за своїми властивостями добре відомий доказово стійкий генератор Blum-Blum-Shub (BBS). У той же час у роботі [12] виявлений суттєвий недолік – генератор GPSSD не забезпечує формування послідовностей максимального періоду. У роботі [11] запропонований вдосконалений метод формування ППВЧ, заснований на введенні в класичну схему GPSSD додаткового етапу формування послідовностей максимального періоду. З одного боку, введена зміна не погіршує статистичних властивостей формованих ППВЧ і зберігає застосовність моделі доказової стійкості, з іншого боку, – забезпечує максимальний період формування послідовностей.

Слід зазначити, що за своєю структурою вдосконалений метод реалізується за допомогою простих, обчислювально ефективних операцій і дозволяє реалізувати швидке формування ППВЧ з гарними статистичними властивостями. У той же час значне збільшення довжини періоду ППВЧ може бути досягнуто виключно за рахунок підвищення розмірності секретних ключових даних, що істотно ускладнює процедуру рівноважного кодування [11]. ***Перспективним напрямом досліджень*** у цьому сенсі є розробка методу швидкого формування ППВЧ доказової стійкості з підвищеною довжиною періоду формованих послідовностей.

Основна частина

1. Терміни і визначення алгебраїчної теорії надмірного кодування і формулювання теоретико-складностної задачі декодування випадкового коду. Введемо основні терміни і визначення, які використовуються в теорії надмірного кодування [10, 11], розглянемо основні аналітичні співвідношення і сформулюємо теоретико-складностну задачу декодування випадкового коду.

Зафіксуємо скінчене поле $GF(q)$. Розглянемо векторний простір $GF^n(q)$ як множину n – послідовностей елементів з $GF(q)$ з компонентним складанням та множенням на скаляр. *Лінійний* (n, k, d) *код* V є підпростором $GF^k(q)$ у просторі $GF^n(q)$, тобто не порожня безліч n – послідовностей (*кодових слів*) над $GF(q)$; k – *розмірність* лінійного підпростору; d – *мінімальна кодова відстань* (мінімальна вага ненульового кодового слова). Величину $R = k/n$ називають *відносною швидкістю коду*, величину $\delta = d/n$ – *відносною мінімальною кодовою відстанню*.

Лінійний код як лінійний підпростір в $GF^n(q)$ однозначно задається набором базисних векторів – *породжувальною матрицею* G коду V, тобто матрицею рангу $\mathrm{rank}(G) = k$, розмірності $k \times n$. Будь-яке кодове слово є лінійною комбінацією рядків з G. Для кодування може використовуватися будь-яка взаємо однозначна відповідність інформаційних k – послідовностей і n – послідовностей кодових слів, задаючих відображення

$$\varphi : GF^k(q) \to GF^n(q).$$

Найбільш проста відповідність інформаційного k – розрядного *інформаційного слова*

$$I = (I_0, \ I_1 \ , ..., \ I_{k-1}); \ I_i \in GF(q); \quad i = 0, 1, ..., k-1$$

і n – розрядного кодового слова

$$C = (C_0 \ \ C_1 \ \ ... \ \ C_{n-1}); \ C_i \in GF(q); \ i = 0, 1, ..., n-1$$

задається виразом $C = I \cdot G$.

Лінійний підпростір, що ототожнює код V, має ортогональне доповнення, базис якого задається *перевірочною матрицею* H коду V, тобто матрицею рангу $\mathrm{rank}(H) = r, \ r = n - k$.

Розмірність перевірочної матриці $r \times n$, причому

$$G \cdot H^T = 0,$$

де під «0» розуміється $k \times r$ матриця нульових елементів з $GF(q)$.

Якщо розглядати матрицю H як набір базисних векторів деякого лінійного підпростору, отримаємо лінійний код $V^{\perp}$, що є дуальним до V. Довільна n – послідовність

$$C = (C_0, \ C_1 \ , ..., \ C_{n-1})$$

є кодовим словом коду V у тому випадку, коли вона ортогональна кожному рядку перевірочної матриці H, тобто $C \cdot H^T = 0$.

Вектор $S = (S_0, \ S_1 \ , ..., \ S_{r-1}), \ S_i \in GF(q), \quad i = 0, 1, ..., r-1,$

Який називається в теорії кодування *синдромом*, може бути обчислений множенням кодового слова з помилками $C^* = C + E$ на транспоновану перевірочну матрицю H коду V:

$$S = C^* \cdot H^T = C \cdot H^T + E \cdot H^T = E \cdot H^T,$$

де E – вектор помилок:

$$E = (E_0 \ \ E_1 \ \ ... \ \ E_{n-1}); \ E_i \in GF(q); \quad i = 0, 1, ..., n-1;$$

C^* – спотворене помилками кодове слово:

$$C^* = (C^*_0 \ \ C^*_1 \ \ ... \ \ C^*_{n-1}); \ C^*_i \in GF(q); \quad i = 0, 1, ..., n-1.$$

Отже, значення синдрому S залежить тільки від вектора помилок E і не залежить від кодового слова C.

Завдання декодування (n, k, d) коду V над $GF(q)$ полягає в знаходженні кодового слова C за відомими матрицями G і H і кодовим словом з помилками C^*. З урахуванням вищевикладеного, завдання декодування можна переформулювати таким чином: знайти вектор помилок E якщо відома синдромна послідовність S.

У загальному випадку, для випадкового лінійного коду, тобто для коду з випадково незалежними і рівноімовірно вибраними k лінійно незалежними векторами з $GF^n(q)$ створюючими базис лінійного підпростору $GF^k(q) \subseteq GF^n(q)$, сформульоване вище завдання суть теоретико-складностне завдання декодування випадкового коду. Складність його рішення, наприклад, кореляційним способом, тобто за допомогою зіставлення кодового слова з помилками C^* з усіма кодовими словами C коду (n, k, d) над V росте $GF(q)$ експоненціально від параметрів коду (для повного перебирання кодових слів буде потрібно q^k спроб).

З використанням уведених визначень і позначень теорії надмірного кодування нижче пропонується метод швидкого формування ППВЧ доказової стійкості. Він заснований на застосуванні обчислювально ефективних алгоритмів надмірного кодування і дозволяє за рахунок зведення відновлення секретних ключових даних до рішення теоретико-складностної задачі декодування випадкового коду, забезпечити високу криптографічну стійкість синтезованих генераторів ППВЧ.

2. Розробка методу швидкого формування ППВЧ доказової стійкості. Для формування ППВЧ з високою довжиною періоду і зведенням завдання криптоаналізу до декодування випадкового коду за відомими кодовими словами з помилками, як функції від секретного вектора-ключа, пропонується метод, що є сукупністю прийомів і операцій алгебраїчного кодування блоковими кодами, неалгебраїчного кодування рівноважними нелінійними кодами, комбінаторики і теорії полів Галуа. Суть пропонованого методу швидкого формування ППВЧ полягає в псевдовипадковому формуванні кодових слів надмірного блокового коду і рівноважних посилок, які виступають як одноразові сеансові ключі, порозрядному складанні відповідних послідовностей і зведенні завдання відновлення секретних ключових даних до декодування випадкового коду. Структура пропонованого методу складається з таких етапів.

Етап псевдовипадкового формування кодових слів надмірного блокового коду. На цьому етапі з використанням методів лінійної алгебри, методів перешкодостійкого кодування лінійними блоковими кодами формуються кодові слова надмірного блокового коду. Для цього випадково, рівноімовірно і незалежно від інших абонентів інформаційного обміну формуються секретні ключові дані, які задають параметри роботи алгоритму формування інформаційних послідовностей надмірного блокового коду.

Нехай $K = \left\{K_1, K_2, ..., K_{q^k}\right\}$ – безліч секретних ключів, $|K| = q^k$, де $K_i = \left(K_{i_0}, K_{i_1}, ..., K_{i_{k-1}}\right)$; $K_i \in K$; $K_{i_j} \in GF(q)$.

Тоді вхідні (інформаційні) послідовності надмірного лінійного блокового коду утворюють безліч значень (образів)

$$I_K = \left\{I_{K_1}, I_{K_2}, ..., I_{K_{q^k}}\right\}$$

такого відображення: $\varphi : K \to I_K$,

де $I_{K_i} = \varphi(K_i) = \left(I_{Ki_0}, I_{Ki_1}, ..., I_{Ki_{k-1}}\right)$; $I_{Ki} \in I_K$;

$$I_{Ki_j} \in GF(q).$$

У простому випадку $K = I_K$, тобто елементи безлічі секретних ключів збігаються з елементами безлічі інформаційних послідовностей надмірного блокового коду.

Алгоритм послідовного формування інформаційних послідовностей може бути реалізований різними способами, наприклад, з використанням лінійних рекурентних регістрів (ЛРР), де початкове заповнення регістра відповідає значенню введених секретних ключових даних. Структурна схема пристрою формування інформаційних послідовностей надмірного блокового коду з використанням ЛРР у конфігурації Галуа наведена на рис. 1.

Пристрій, структурна схема якого наведена на рис. 1, функціонує таким чином. Протягом перших k часових відліків ключ (перемикач) знаходиться у верхньому положенні, а регістр зсуву заповнюється ключовою послідовністю

$$K_i = \left(K_{i_0}, K_{i_1}, ..., K_{i_{k-1}}\right).$$

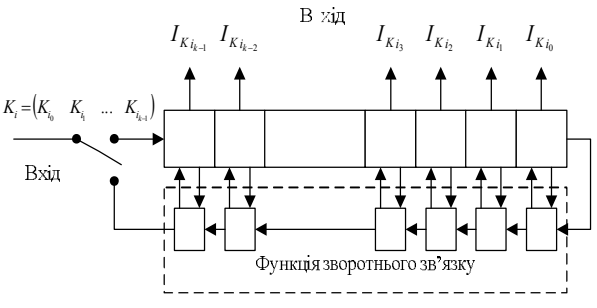

Рис. 1. Структурна схема формування інформаційних послідовностей надмірного коду

Протягом подальших $q^k - 1$ часових відліків ключ (перемикач) знаходиться в нижньому положенні, і на вихід пристрою подаються значення, що зберігаються в осередках регістра зсуву. На кожно-

му часовому інтервалі інформація, що зберігається в регістрі зсуву переміщається на один осередок управо, а по ланцюгу зворотного зв'язку надходить значення, що зберігається в крайньому правому осередку. Функція зворотного зв'язку задає конкретний вид комутацій ланцюга зворотного зв'язку і забезпечує формування псевдовипадкової послідовності максимального періоду.

Наступною операцією на першому етапі пропонованого методу є псевдовипадкове формування кодових слів надмірного блокового коду, тобто реалізується відображення

$$\phi : I_K \to C_K, \qquad \text{де}$$

$$C_K = \left\{ C_{K1}, C_{K2}, ..., C_{K_{q^k}} \right\}_-$$

безліч кодових слів надмірного коду, тобто

$$C_{K_i} = \phi\left(I_{K_i}\right) = \left(C_{Ki_0}, \quad C_{Ki_l} \quad ,..., \quad C_{Ki_{n-1}}\right),$$

$$C_{Ki} \in C_K \subseteq GF^n(q), \; C_{Ki_j} \in GF(q).$$

Правило надмірного кодування задає конкретний вид відображення $\phi : I_K \to C_K$ і визначається, виходячи з міркувань простоти практичної реалізації перешкодостійкого кодування лінійними блоковими кодами. Ця операція може бути реалізована одним із відомих способів надмірного кодування, наприклад, за допомогою цифрового рекурсивного фільтра (рис. 2).

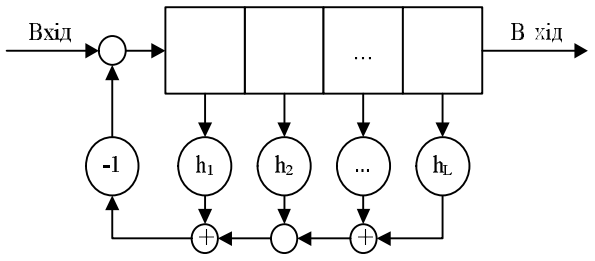

Рис. 2. Цифровий рекурсивний фільтр

Якщо на вхід цифрового рекурсивного фільтру подати послідовність символів

$$\{i_k, \quad ... \quad i_1, \quad i_0\},$$

то на виході отримаємо послідовність

$$\{c_k, \quad ... \quad c_1, \quad c_0\},$$

яка задовольняє рекурсії [13, 14]

$$c_j = -\sum_{i=1}^{L} h_i i_{j-i} + i_j.$$

Таким чином, у результаті виконання перелічених операцій першого етапу пропонованого методу кодові слова

$$C_{Ki} = \left(C_{Ki_0}, \quad C_{Ki_l} \quad ,..., \quad C_{Ki_{n-1}}\right)$$

надмірного коду з множини

$$C_K = \left\{ C_{K1}, C_{K2}, ..., C_{K_{q^k}} \right\}$$

формуються псевдовипадково, відповідно до сформованих інформаційних послідовностей

$$I_{Ki} = \left(I_{Ki_0}, \quad I_{Ki_l} \quad ,..., \quad I_{Ki_{k-1}}\right)$$

з множини

$$I_K = \left\{ I_{K1}, I_{K2}, ..., I_{K_{q^k}} \right\}.$$

Кожен елемент множини I_K формується псевдовипадково, з використанням правил формування послідовностей максимального періоду за введеним ключем

$$K_i = \left(K_{i0}, \quad K_{i1} \quad ,..., \quad K_{ik-1}\right)$$

з множини

$$K = \left\{ K_1, K_2, ..., K_{q^k} \right\}.$$

Розглянемо другий етап пропонованого методу формування ППВЧ.

Етап псевдовипадкового формування сеансових ключових даних. На цьому етапі з використанням методів перешкодостійкого кодування нелінійними блоковими кодами формуються рівноважні кодові послідовності, які використовуються при формуванні ППВЧ як сеансові ключові дані. Для цього випадково, рівноімовірно і незалежно від інших абонентів інформаційного обміну формуються секретні ключові дані, які задають параметри роботи алгоритму рівноважного кодування.

Нехай

$$K^* = \left\{ K^*_1, K^*_2, ..., K^*_M \right\} -$$

множина секретних ключів $|K^*| = M$,

де

$$M = q^m,$$

$$m = \left\lfloor \log_q\left(C_n^w\right) \right\rfloor;$$

$$C_n^w = \frac{n!}{w! \cdot (n-w)!};$$

n – довжина рівноважної послідовності;

w – заздалегідь задане значення ваги послідовності, тобто число ненульових елементів послідовності сеансових ключів

$$K^*_i = \left(K^*_{i_0}, \quad K^*_{i_l} \quad ,..., \quad K^*_{i_{m-1}}\right),$$

$$K^*_i \in K^*; \; K^*_{i_j} \in GF(q).$$

Тоді вхідні (інформаційні) послідовності надмірного рівноважного блокового коду утворюють множину значень (образів)

$$I^*_K = \left\{ I^*_{K1}, I^*_{K2}, ..., I^*_{KM} \right\}$$

такого відображення:

$$\varphi^* : K^* \to I^*_K,$$

де

$$I^*_{K_i} = \varphi^*\left(K^*_i\right) = \left(I^*_{Ki0}, \quad I^*_{Kil} \quad ,..., \quad I^*_{Kim-1}\right);$$

$$I^*_{Ki} \in I^*_K, \; I^*_{Ki_j} \in GF(q).$$

У простому випадку

$$K^* = I^*_K,$$

тобто елементи множини секретних ключів збігаються з елементами безлічі інформаційних послідовностей надмірного рівноважного блокового коду.

Алгоритм послідовного формування інформаційних послідовностей може бути реалізований різними способами, наприклад, з використанням ЛРР (рис. 1), де початкове заповнення регістра відповідає значенню введених секретних ключових даних.

Наступною операцією на другому етапі пропонованого методу є псевдовипадкове формування кодових слів надмірного рівноважного блокового коду. З використанням алгоритмів рівноважного кодування здійснюється перетворення вхідних послідовностей рівноважного коду в послідовність сеансових ключів, тобто здійснюється відображення $\gamma : I^*_K \to S_K$, де $S_K = \left\{S_{K1}, S_{K2}, ..., S_{K_q{}^m}\right\}$ – множина рівноважних послідовностей, тобто множина кодових слів рівноважного коду

$$S_{K_i} = \gamma\left(I^*_{Ki}\right) = \left(S_{Ki_0}, \quad S_{Ki_1} \quad ,..., \quad S_{Ki_{n-1}}\right);$$

$$S_{Ki} \in S_K \subseteq GF^n\left(q\right);$$

$$S_{Ki_j} \in GF\left(q\right), \; w\left(S_{Ki}\right) = w.$$

Алгоритми рівноважного кодування детально розглянуті в [15].

Наступною операцією другого етапу пропонованого методу є псевдовипадкове формування сеансових ключових даних. Для цього над сформованими рівноважними послідовностями (кодовими словами рівноважного коду)

$$S_{Ki} = \left(S_{Ki_0}, \quad S_{Ki_1} \quad ,..., \quad S_{Ki_{n-1}}\right) \in S_K = \left\{S_{K1}, S_{K2}, ..., S_{K_q{}^m}\right\}$$

виконується узагальнено-переставне перетворення, що не змінює вагових характеристик коду і, в той же час додає властивість стохастичності формованих сеансових ключів.

Формалізовано процес формування сеансових ключів запишемо у вигляді відображення

$$\psi : S_K \to S^*_K,$$

де

$$S^*_K = \left\{S^*_{K1}, S^*_{K2}, ..., S^*_{K_q{}^m}\right\} -$$

множина сеансових ключів - рівноважних послідовностей, отриманих в результаті узагальненого-переставного перетворення

$$S^*_{K_i} = \psi\left(S_{K_i}, \Lambda\right) = S_{K_i} \cdot \Lambda^T,$$

де $S_K \cdot \Lambda^T$ – матричне множення вектора–рядка S_K довжиною n елементів з $GF\left(q\right)$ на транспоновану квадратну $n \times n$ узагальнено-переставну матрицю Λ.

Результатом останньої операції є рівноважний вектор

$$S^*_{Ki} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad ... \quad S^*_{Ki_{n-1}}\right),$$

де

$$S^*_{Ki} \in S^*_K \subseteq GF^n\left(q\right),$$

$$S^*_{Ki_j} \in GF\left(q\right), \; w\left(S^*_{Ki}\right) = w.$$

Узагальнено-переставна матриця Λ, яка задає правило формування сеансових ключів, виступає як довготривалий ключ.

Розглянемо третій етап пропонованого методу формування ППВЧ.

Етап формування ППВЧ. У результаті виконання основних операцій першого і другого етапів пропонованого методу побудови ППВЧ псевдовипадково сформовані кодові слова

$$C_{Ki} = \left(C_{Ki_0}, \quad C_{Ki_1} \quad ,..., \quad C_{Ki_{n-1}}\right)$$

надмірного коду і сеансові ключі

$$S^*_{Ki} = \left(S^*_{Ki_0} \quad S^*_{Ki_1} \quad ... \quad S^*_{Ki_{n-1}}\right) -$$

рівноважні псевдовипадкові послідовності.

На третьому, завершальному етапі формування ППВЧ отримані послідовності C_{Ki} і S^*_{Ki} з елементами з $GF\left(q\right)$ поелементно складаються в арифметиці кінцевого поля $GF\left(q\right)$. Формалізовано запишемо це перетворення у вигляді відображення:

$$\xi : \left(S^*_K\right) \times \left(C_K\right) \to C^*_K,$$

де

$$C^*_K = \left\{C^*_{K1}, C^*_{K2}, ..., C^*_{K_q{}^{m+k}}\right\};$$

$$\left|C^*_K\right| = \left|S^*_K\right| \cdot \left|C_K\right| = q^m \cdot q^k = q^{m+k}.$$

Множина C^*_K – шукана безліч фрагментів формованої ППВЧ,

де $C^*_{Ki} = \left(C^*_{Ki_0} \quad C^*_{Ki_1} \quad ... \quad C^*_{Ki_{n-1}}\right);$

$$C^*_{Ki} \in C^*_K \subseteq GF^n\left(q\right),$$

$$C^*_{Ki_j} = \left(S^*_{Ki_j} + C_{Ki_j}\right) \in GF\left(q\right).$$

Сформований в результаті виконання операцій методу фрагмент ППВЧ що є результатом декількох функціональних відображень, в загальному вигляді запишемо:

$$\tilde{N}^*_{K_i} = \xi\left(S^*_{K_i}, \tilde{N}_{K_i}\right) = \xi\left(\psi\left(S_{K_i}, \Lambda\right), \phi\left(I_{K_i}\right)\right) =$$

$$= \xi\left(\psi\left(\gamma\left(\varphi^*\left(K^*_i\right)\right), \Lambda\right), \phi\left(\varphi\left(K_i\right)\right)\right).$$

Знаходження ключових даних K_i і/або K^*_i за відомим (перехопленим) фрагментом ППВЧ $C^*_{K_i}$ пов'язано з пошуком обчислювально ефективних алгоритмів виконання зворотного відображення $\xi^{-1}\left(C^*_{K_i}\right)$.

Аналіз основних положень алгебраїчної теорії блокових кодів, досвід побудови і застосування систем надмірного кодування перешкодостійкими кодами показує, що це завдання еквівалентне теоретико-складностному завданню декодування випадкового коду, тобто відповідає математичному завданню, сформульованому в попередньому пункті даної статті.

Таким чином, у результаті проведених досліджень розроблений метод формування ППВЧ,

виконання всіх етапів якого дозволяє за заданими ключовими даними K_i, K^*_i і за уведеним довготривалим ключем – узагальнено-переставній матриці Λ за кінцеве число кроків формувати ППВЧ, із зведенням завдання криптоаналізу до рішення теоретико-складностної задачі декодування випадкового коду за відомим кодовим словом з помилками як функції від секретного вектора-ключа. Період формованої ППВЧ дорівнює:

$$L = l_1 \cdot l_2 = \left(q^k - 1\right) \cdot \left(q^m - 1\right),$$

де l_1 і l_2 – взаємопрості довжини періодів кодових слів вживаних надмірних кодів, правила формування яких задаються відповідно на першому і другому етапах запропонованого методу.

3. Дослідження стійкості запропонованого методу. Проведемо дослідження стійкості запропонованого методу формування ППВЧ до криптографічних атак супротивника, заснованих на використанні алгоритмів декодування надмірних (n, k, d) кодів над GF(q).

Криптографічну стійкість визначимо як обчислювальну складність найбільш ефективних атак, тобто оцінку стійкості проводитимемо за критерієм мінімального риску:

$$Q = \min\left\{N_i\right\}, i = 1..L,$$

де N_i – обчислювальна складність і-го методу криптоаналізу; L – кількість відомих методів криптоаналізу для даного криптоалгоритму.

В результаті проведених досліджень отриманий наступний аналітичний вираз:

$$Q = \min\left\{\begin{array}{c} q^k, \\ 2 \cdot \sum_{i=1}^{t} (q-1)^i \cdot \frac{n!}{i! \cdot (n-i)!}, \\ \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \cdots \left\lceil \frac{n-t-1}{n-k-t-1} \right\rceil \right\rceil \right\rceil \end{array}\right\},$$

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

На рис. 3. наведені залежності складності реалізації атак, заснованих на таких алгоритмах:

1) алгоритмі кореляційного декодування $N_{\hat{e}.\ddot{a}.}(R)$;

2) алгоритмі синдромного декодування $N_{\tilde{n}.\ddot{a}.}(R)$;

3) алгоритмі перестановочного декодування $N_{\ddot{i}.\ddot{a}.}(R)$ для $q = 2$ і $n = 1000$.

Аналіз залежностей, приведених на рис. 3, показує, що застосування розглянутих атак при $0{,}1 \le R \le 0{,}95$ і довжині використовуваної коди $n = 1000$ обчислювально недоцільно, забезпечувана стійкість задовольняє сучасним вимогам.

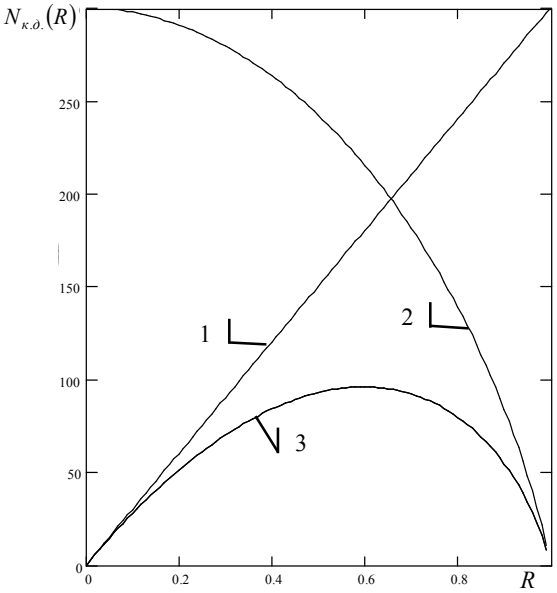

Рис. 3. Залежності обчислювальної складності різних методів крипто аналізу для $q = 2$:
1) $N_{\hat{e}.\ddot{a}.}(R)$, 2) $N_{\tilde{n}.\ddot{a}.}(R)$, 3) $N_{\ddot{i}.\ddot{a}.}(R)$

Таким чином, проведені дослідження показали, що розроблений метод формування ППСЧ володіє високими показниками стійкості. Теоретична оцінка складності криптоаналізу показала, що застосування методів алгебри декодування при відповідних параметрах кодових конструкцій не дозволяє супротивникові ефективно реалізувати криптоаналіз запропонованих генераторів.

Висновки

У ході проведених досліджень вперше запропонований метод швидкого формування доказово стійких ППВЧ, в якому за рахунок використання двох векторів секретних ключових даних вдається при незмінній розрядності рівноважних векторів істотно збільшити довжину періоду формованих ППВЧ.

Встановлено, що виконання всіх етапів запропонованого методу дозволяє за заданими ключовими даними за кінцеве число кроків формувати ППВЧ, причому завдання криптоаналізу зведиться до розв'язання теоретико-складностної задачі декодування випадкового коду за відомим кодовим словом з помилками як функції від секретного вектора-ключа.

Основною перевагою запропонованого методу перед методом GPSSD [5] і вдосконаленим методом [11] є збільшення довжини періоду формованих ППВЧ.

Перспективним ***напрямом*** подальших досліджень є розробка практичних рекомендацій щодо впровадження отриманих результатів, дослідження обчислювально ефективних алгоритмів рівноважного кодування недвійкових послідовностей.

Список літератури

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

2. Поповский В.В. Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков; Харьковский национальный университет радиоэлектроники. – Х.: ООО "Компания Смит", 2006. – 238 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Издательство ТРИУМФ, 2002 – 816 с.

4. Аунг Т.М. Разработка и исследование стохастических методов защиты программных систем: автореф. дисс. ... канд. техн. наук: 05.13.11, 05.13.19 / Т.М. Тунг; Московский инженерно-физический институт (государственный университет). – М., 2007. – 20 с.

5. Fisher Jean-Dernard , Jacques Stern. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245 – 255.

6. Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. – СПб.: АНО НПО Профессионал, 2005. – 478 с.

7. Рябко Б.Я. Криптографические методы защиты информации: /Б.Я.Рябко, А.Н.Фионов. – М: Горячая линия – Телеком, 2005. – 229 с.

8. Фергюсон Н. Практическая криптография /Н.Фергюсон, Б.Шнаер. – М.: Издательский дом Вильямс, 2005. – 424 с.

9. Кузнецов А.А. Исследование статистической безопасности генераторов псевдослучайных чисел / А.А. Кузнецов, Р.В. Королев, Ю.Н. Рябуха // Системи обробки інформації. – Х., 2008. – Вип. 3(70). – С. 79-82.

10.Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag, 829 p.

11.Кузнецов А.А. Усовершенствованный метод быстрого формирования последовательностей псевдослучайных чисел / А.А. Кузнецов, Р.В. Королев, Ю.Н.Рябуха // Збірник наукових праць ХУ ПС. – Х., 2008. – Вип. 3(18). – С. 101-104.

12.Корольов Р.В. Дослідження періодичних властивостей генераторів псевдовипадкових чисел, заснованих на використанні надмірних блокових кодів / Р.В. Корольов // Системи озброєння і військова техніка. – Х., 2008. – № 3(15). – С. 126-128.

13.Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки./ Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

14.Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

15.Методи та алгоритми адаптивного рівноважного кодування на основі біноміальних чисел для інформаційних систем: автореф. дис. / О.В. Бережная; Харк. нац. ун-т радіоелектрон. – Х., 2002. – С. 19. – [Електронний ресурс] Режим доступу до автореф.: http://disser.com.ua/ contents/31551/html.

16.Кларк Дж Кодирование с исправлением ошибок в системах цифровой связи /Дж.Кларк, Дж.Кейн. – М.: Радио и связь, 1987. – 391 с.

Надійшла до редколегії 11.11.2008

Рецензент: д-р. техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД БЫСТРОГО ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ДОКАЗУЕМОЙ СТОЙКОСТИ

А.А. Кузнецов, Р.В. Корольов, Ю.М. Рябуха

Рассматриваются методы формирования последовательностей псевдослучайных чисел (ППСЧ), исследуется подход к построению доказуемо стойких генераторов, стойкость которых основана на теоретико-сложностной проблеме синдромного декодирования. Предлагается метод быстрого формирования ППСЧ доказуемой стойкости, который позволяет обеспечить максимальный период формируемых последовательностей. Проводится исследование стойкости предложенного метода формирования ППСЧ к криптографическим атакам противника, основанным на использовании алгоритмов декодирования избыточных (n, k, d) кодов над GF(q).

Ключевые слова: *последовательности псевдослучайных чисел, генератор псевдослучайных чисел.*

METHOD OF RAPID FORMING OF SEQUENCES PSEUDO-RANDOM NUMBERS OF DEMONSTRABLE FIRMNESS

A.A. Kyznetcov, R.V. Korol'ov, Yu.M. Ryabukha

The methods of forming of sequences of pseudo-random numbers (PRN) are examined, going is probed near a construction demonstrable proof generators firmness of which is based on theorist of intricate problem of the syndromic decoding. The method of the rapid forming of PRN of demonstrable firmness is offered, which allows to provide the maximal period of the formed sequences. Research of firmness of the offered method of forming of PRN is conducted to the cryptographic attacks of opponent, to based on the use of decoding of surplus (n,k, d) kodas algorithms above GF(q).

Keywords: *numbers sequence of pseudo-random numbers , generator of pseudocasual numbers.*